



UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
09/830,392	06/18/2001	Yoshihito Ishibashi	450108-02659	6916

20999 7590 06/27/2005

FROMMER LAWRENCE & HAUG
745 FIFTH AVENUE- 10TH FL.
NEW YORK, NY 10151

EXAMINER

DADA, BEEMNET W

ART UNIT PAPER NUMBER

2135

DATE MAILED: 06/27/2005

Please find below and/or attached an Office communication concerning this application or proceeding.

Office Action Summary	Application No. 09/830,392	Applicant(s) ISHIBASHI ET AL.	
	Examiner Beemnet W. Dada	Art Unit 2135	

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --
Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE 3 MONTH(S) FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If the period for reply specified above is less than thirty (30) days, a reply within the statutory minimum of thirty (30) days will be considered timely.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

Status

- 1) ☒ Responsive to communication(s) filed on 13 April 2005.
2a) ☒ This action is **FINAL**. 2b) ☐ This action is non-final.
3) ☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims

- 4) ☒ Claim(s) 69-117 and 148-170 is/are pending in the application.
4a) Of the above claim(s) 118-147 and 171-218 is/are withdrawn from consideration.
5) ☐ Claim(s) _____ is/are allowed.
6) ☒ Claim(s) 69-117 and 148-170 is/are rejected.
7) ☐ Claim(s) _____ is/are objected to.
8) ☐ Claim(s) _____ are subject to restriction and/or election requirement.

Application Papers

- 9) ☐ The specification is objected to by the Examiner.
10) ☐ The drawing(s) filed on _____ is/are: a) ☐ accepted or b) ☐ objected to by the Examiner.
Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).
Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).
11) ☐ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

Priority under 35 U.S.C. § 119

- 12) ☐ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).
a) ☐ All b) ☐ Some * c) ☐ None of:
1. ☐ Certified copies of the priority documents have been received.
2. ☐ Certified copies of the priority documents have been received in Application No. _____.
3. ☐ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

* See the attached detailed Office action for a list of the certified copies not received.

Attachment(s)

- | | |
|--|---|
| 1) <input checked="" type="checkbox"/> Notice of References Cited (PTO-892) | 4) <input type="checkbox"/> Interview Summary (PTO-413)
Paper No(s)/Mail Date. _____ |
| 2) <input type="checkbox"/> Notice of Draftsperson's Patent Drawing Review (PTO-948) | 5) <input type="checkbox"/> Notice of Informal Patent Application (PTO-152) |
| 3) <input type="checkbox"/> Information Disclosure Statement(s) (PTO-1449 or PTO/SB/08)
Paper No(s)/Mail Date _____ | 6) <input type="checkbox"/> Other: _____ |

DETAILED ACTION

1. This office action is in reply to an amendment filed on April 13, 2005. Claims 69-71, 75, 79, 83, 87, 91, 95-97, 101, 104, 108, 111, 115, 148-150, 157 and 164 have been amended. Claims 69-117 and 148-170 have been examined.

Claim Objections

2. Claim 83 is objected to because of the following informalities: in line 5 of claim 83 the word data is cancelled. Appropriate correction is required.

Claim Rejections - 35 USC § 102

3. The following is a quotation of the appropriate paragraphs of 35 U.S.C. 102 that form the basis for the rejections under this section made in this Office action:

A person shall be entitled to a patent unless –

(e) the invention was described in (1) an application for patent, published under section 122(b), by another filed in the United States before the invention by the applicant for patent or (2) a patent granted on an application for patent by another filed in the United States before the invention by the applicant for patent, except that an international application filed under the treaty defined in section 351(a) shall have the effects for purposes of this subsection of an application filed in the United States only if the international application designated the United States and was published under Article 21(2) of such treaty in the English language.

4. Claim 69-71, 75, 79, 83, 87 and 91 are rejected under 35 U.S.C. 102(e) as being anticipated by Wool US Patent 6,073,122.
5. As per claims 69-71, 75, 79, 83, 87 and 91, Wool teaches an information distribution system for distributing data from an information sending device to an information receiving device [see abstract],
- wherein said information sending device (i.e., headend server) comprises:

sending means for sending a plurality of distribution keys, each corresponding to a predetermined time period and send data, which includes data encrypted with key data [column 4, lines 1-16, 20-25 and column 5, lines 40-61];

said information receiving device comprises:

receiving means for receiving send data and said plurality of distribution keys and receiving end controlling means for decrypting said encrypted data [column 6, lines 41-60 and column 5, lines 40-61];

wherein each of said plurality of distribution keys allows decryption of said encrypted data within the predetermined time period associated with said distribution key, independent of a connection during said predetermined time period associated with said distribution key (i.e., during a given billing period) [column 4, lines 3-5, 62-67 and figures 5-7].

Claim Rejections - 35 USC § 103

6. The following is a quotation of 35 U.S.C. 103(a) which forms the basis for all obviousness rejections set forth in this Office action:

(a) A patent may not be obtained though the invention is not identically disclosed or described as set forth in section 102 of this title, if the differences between the subject matter sought to be patented and the prior art are such that the subject matter as a whole would have been obvious at the time the invention was made to a person having ordinary skill in the art to which said subject matter pertains. Patentability shall not be negated by the manner in which the invention was made.

7. Claims 72-74, 76-78, 80-82, 84-86, 88-90 and 92-94 are rejected under 35 U.S.C. 103(a) as being unpatentable over Wool US Patent 6,073,122 in view of Horne US Patent 4,887,296.

8. As per claims 72-74, 76-78, 80-82, 84-86, 88-90 and 92-94, Wool teaches an information distribution system as applied above. Wool is silent on the key data being individual

Art Unit: 2135

key that is specific to a device and said key data that is periodically updated. However, the system of generating encryption/decryption keys that are specific to a device and are periodically updated is old and well known in the art. For example, within the same field of endeavor Horne teaches a cryptographic system for data transmission, including a method for providing individual keys that are specific to a device [column 3, lines 63 – column 4, lines 14], and further, including periodically changing keys at a time interval [column 4, lines 41-44], which has the advantage of transmitting data only to a specific authorized device securely. Therefore it would have been obvious to one having ordinary skill in the art at the time the invention was made to employ the teachings of Horne within the system of Wool in order to further enhance the security of the system by changing keys periodically and providing individual keys as taught by Horne.

9. Claim 95-117 and 148-170 are rejected under 35 U.S.C. 103(a) as being unpatentable over Richards US Patent 6,690,795 B1 in view of Horne US Patent 4,887,296 and further in view of Wool US Patent 6,073,122.

10. As per claims 95-117, Richards teaches an information distribution system for distributing predetermined content data from an information sending device to an information receiving device [see abstract] characterized in that:

said information sending device comprises: sending end controlling means for encrypting content data with a key SK [column 8, lines 37-43], and encrypting the key SK with a second key PK [column 9, lines 14-16]; and encrypting the second key PK with a predetermined third key (Customer Code) [column 9, lines 16-17], and transmitting the

Art Unit: 2135

encrypted content, encrypted content key and encrypted second key PK [column 9, lines 19-25 and column 8, lines 31-42].

said information receiving device comprises: receiving means for receiving the encrypted content encrypted with the content key (SK), the control key encrypted with the second key (PK) and the encrypted second key [column 9, lines 19-25 and column 8, lines 31-42]; and receiving end controlling means for decrypting the second key (PK) with the third key (Customer Code) that is given in advance, and decrypting the content key (SK) with the decrypted second key (PK), and decrypting the content with the content key [column 9, lines 24-44]. Furthermore, Richards teaches periodically changing content key (SK) and second key (PK) [column 8, lines 32-35]. Richards is silent on the second key being individual key that is specific to a device. However, within the same field of endeavor Horne teaches a cryptographic system for data transmission, including a method for providing individual keys that are specific to a device, wherein the individual keys encrypt content key used for encrypting content [column 3, lines 63 – column 4, lines 14], and further, including periodically changing keys at a time interval [column 4, lines 41-44], which has the advantage of transmitting data only to a specific authorized device securely. Therefore it would have been obvious to one having ordinary skill in the art at the time the invention was made to employ the teachings of Horne within the system of Richards in order to further enhance the security of the system by providing individual keys as taught by Horne. Furthermore, Wool teaches plurality of distribution keys, each distribution key corresponding to a predetermined time period and allowing decryption of individual key (for example program key) within the predetermined time period associated with said distribution key, independent of connection during said predetermined time period associated with said distribution key [column 4, lines 1-16, 20-25 and column 5, lines 40-61 and figures 5-7]. Both Richards-Horne and Wool teach an information distribution system. It would have been obvious to one having ordinary skill

Art Unit: 2135

in the art at the time of applicant's invention to employ the teachings of Wool within the combination of Richards and Horne in order to further allow plurality of keys to encrypt/decrypt multiple packages of content and allow use of the content for a predetermined billing period.

11. As per claims 148-170, Richards teaches an information distribution system for distributing predetermined content data from an information sending device to an information receiving device [see abstract] characterized in that:

said information sending device comprises: sending end controlling means for encrypting content data with a key SK [column 8, lines 37-43], and encrypting the key SK with a second key PK [column 9, lines 14-16]; and encrypting the second key PK with a predetermined third key (Customer Code) [column 9, lines 16-17], and transmitting the encrypted content, encrypted content key and encrypted second key PK [column 9, lines 19-25 and column 8, lines 31-42].

said information receiving device comprises: receiving means for receiving the encrypted content encrypted with the content key (SK), the control key encrypted with the second key (PK) and the encrypted second key [column 9, lines 19-25 and column 8, lines 31-42]; and receiving end controlling means for decrypting the second key (PK) with the third key (Customer Code) that is given in advance, and decrypting the content key (SK) with the decrypted second key (PK), and decrypting the content with the content key [column 9, lines 24-44]. Furthermore, Richards teaches periodically changing content key (SK) and second key (PK) [column 8, lines 32-35], including changing keys SK and PK after the content has been decrypted [column 9, lines 40-51]. Richards is silent on the second key being individual key that is specific to a device. However, within the same field of endeavor Horne teaches a cryptographic system for data transmission, including a method for providing individual keys that are specific to a device,

Art Unit: 2135

wherein the individual keys encrypt content key used for encrypting content [column 3, lines 63 – column 4, lines 14], and further, including periodically changing keys at a time interval [column 4, lines 41-44], which has the advantage of transmitting data only to a specific authorized device securely. Therefore it would have been obvious to one having ordinary skill in the art at the time the invention was made to employ the teachings of Horne within the system of Richards in order to further enhance the security of the system by providing individual keys as taught by Horne.

The combination of Richards and Horne is silent on plurality of distribution keys, each distribution key corresponding to a predetermined time period. Within the same field of endeavor Wool teaches encrypting a program key with one of a plurality of distribution keys (i.e., package keys) [column 4, lines 1-16, 20-25 and column 5, lines 40-61 and figures 5-7]. Both Richards-Horne and Wool teach an information distribution system. It would have been obvious to one having ordinary skill in the art at the time of applicant's invention to employ the teachings of Wool within the combination of Richards and Horne in order to further allow plurality of keys to encrypt/decrypt multiple packages of content and allow use of the content for a predetermined billing period.

Response to Arguments

12. Applicant's arguments filed on April 13, 2005 have been considered but are moot in view of the new ground(s) of rejection.

Conclusion

13. Applicant's amendment necessitated the new ground(s) of rejection presented in this Office action. Accordingly, **THIS ACTION IS MADE FINAL**. See MPEP § 706.07(a).

Applicant is reminded of the extension of time policy as set forth in 37 CFR 1.136(a).

A shortened statutory period for reply to this final action is set to expire THREE MONTHS from the mailing date of this action. In the event a first reply is filed within TWO MONTHS of the mailing date of this final action and the advisory action is not mailed until after the end of the THREE-MONTH shortened statutory period, then the shortened statutory period will expire on the date the advisory action is mailed, and any extension fee pursuant to 37 CFR 1.136(a) will be calculated from the mailing date of the advisory action. In no event, however, will the statutory period for reply expire later than SIX MONTHS from the date of this final action.

Any inquiry concerning this communication or earlier communications from the examiner should be directed to Beemnet W. Dada whose telephone number is (571) 272-3847. The examiner can normally be reached on Monday - Friday (9:00 am - 5:30 pm).

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Kim Y. Vu can be reached on (571) 272-3859. The fax phone number for the organization where this application or proceeding is assigned is 703-872-9306.

Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see <http://pair-direct.uspto.gov>. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free).

Beemnet Dada

June 20, 2005

ASG
Primary Examiner
Art Unit 2135